

1 BUCHALTER
A Professional Corporation
2 VALERIE BANTNER PEO (SBN: 260430)
425 Market Street, Suite 2900
3 San Francisco, CA 94105
Telephone: 415.227.0900
4 Fax: 415.227.0770
Email: vbantnerpeo@buchalter.com

5 PROSKAUER ROSE LLP
6 Timothy Karcher, Esq. (*pro hac vice* pending)
Nolan Goldberg, Esq.
7 Eleven Times Square
8 New York, NY 10036
Telephone: (212) 969-3000
9 Email: tkarcher@proskauer.com
Email: ngoldberg@proskauer.com

10 Paul Possinger, Esq. (*pro hac vice* pending)
11 70 West Madison, Suite 3800
Chicago, IL 60602-4342
12 Telephone: (312) 962-3550
Email: ppossinger@proskauer.com

13 Attorneys for Berkeley Research Group, LLC
14

15 **UNITED STATES BANKRUPTCY COURT**
16 **NORTHERN DISTRICT OF CALIFORNIA**
17 **SAN FRANCISCO DIVISION**

18 In re
19 THE ROMAN CATHOLIC ARCHBISHOP
20 OF SAN FRANCISCO,
21 Debtor and Debtor in
22 Possession.

Case No. 23-30564

Chapter: Chapter 11

**NOTICE OF DATA SECURITY
INCIDENT**

Judge: Hon. Dennis Montali

23
24
25 **PLEASE TAKE NOTICE** Berkeley Research Group, LLC (“**BRG**”), the Financial
26 Advisor for the Official Committee of Unsecured Creditors in the above-captioned chapter 11
27 case (the “**Case**”) submits as Exhibit A the attached letter (the “**Incident Letter**”) regarding a
28 cybersecurity incident (the “**Incident**”).

1 **PLEASE TAKE FURTHER NOTICE** that, as set forth in the Incident Letter, on March
2 2, 2025, BRG detected suspicious activity in its network and subsequently determined specific
3 BRG internal systems were impacted by ransomware. The Incident, along with containment steps
4 taken by BRG and its advisors, are described in the Incident Letter and attached FAQs.

5 **PLEASE TAKE FURTHER NOTICE** that, since discovery of the Incident, BRG has
6 commenced a thorough investigation, which remains ongoing and will require additional time to
7 complete. BRG has determined, however, that data associated with this case may have been
8 exfiltrated by the threat actor responsible for the Incident. After careful consideration, and with a
9 primary focus on protecting the subjects of any implicated data, BRG reached a settlement with
10 the threat actor, through which the threat actor provided a statement that the data was deleted and
11 would not be distributed. To date, BRG has not detected any evidence of the distribution of any
12 implicated materials.

13 Please refer to the Incident Letter and the annexed FAQs for additional information. All
14 inquiries regarding the Incident should be addressed to: DataAnalysisInquiries@thinkbrg.com.

15
16
17 Dated: May 1, 2025

BUCHALTER, A Professional Corporation

18 By: /s/ Valerie Bantner Peo

Valerie Bantner Peo, Esq.

19 PROSKAUER ROSE LLP

20 Timothy Karcher, Esq. (pro hac vice pending)

21 Nolan Goldberg, Esq.

Paul Possinger, Esq. (pro hac vice pending)

22 Attorneys for Berkeley Research Group, LLC
23
24
25
26
27
28

1 **CERTIFICATE OF SERVICE**

2 I am employed in the County of San Francisco, State of California. I am over the age of
3 18 and not a party to the within action. My business address is at BUCHALTER, A Professional
4 Corporation, 425 Market Street, Suite 2900, San Francisco, CA 94105.

5 On the date set forth below, I served the foregoing document described as:

6
7 • **NOTICE OF DATA SECURITY INCIDENT**

8 on all other parties and/or their attorney(s) of record to this action as follows:

9 **TO BE SERVED BY THE COURT VIA NOTICE OF ELECTRONIC FILING:** The
10 foregoing documents will be served by the court via email and hyperlink to the document. On
11 **May 1, 2025**, I checked the CM/ECF docket for this United States Northern District of California
12 case and determined that the persons listed below are on the Electronic Mail Notice List to
13 receive email notice/service for this case at the email addresses stated below.

- 14 • Mary Alexander malexander@maryalexanderlaw.com
15 • Darren Azman dazman@mwe.com, mco@mwe.com
16 • Jesse Bair jbair@burnsbair.com, kdempski@burnsbair.com
17 • Hagop T. Bedoyan hagop.bedoyan@mccormickbarstow.com, ecf@kleinlaw.com
18 • Jason Blumberg jason.blumberg@usdoj.gov, ustpreion17.sf.ecf@usdoj.gov
19 • Gillian Nicole Brown gbrown@psjlaw.com
20 • John Bucheit jbucheit@phrd.com
21 • Timothy W. Burns tburns@burnsbair.com, kdempski@burnsbair.com
22 • George Calhoun george@ifrahlaw.com
23 • Peter C. Califano pcalifano@nvlawllp.com
24 • Brian P Cawley bcawley@burnsbair.com
25 • Robert M Charles Robert.Charles@wbd-us.com
26 • Jason Chorley jason.chorley@clydeco.us, Robert.willis@clydeco.us
27 • Amanda L. Cottrell acottrell@sheppardmullin.com, JHerschap@sheppardmullin.com
28 • Jennifer Witherell Crastz jcrastz@hemar-rousso.com
• Blaise S Curet bcuret@spcclaw.com
• Melissa M D'Alelio mdalelio@robinskaplan.com
• Jared A. Day jared.a.day@usdoj.gov
• Michele Nicole Detherage mdetherage@robinskaplan.com
• Allan B Diamond adiamond@diamonddmccarthy.com
• Luke N. Eaton lukeeaton@cozen.com, monugiac@pepperlaw.com
• Michael W Ellison mellison@sehlaw.com, kfoster@sehlaw.com
• Stephen John Estey steve@estey-bomberger.com
• Timothy W. Evanston tevanston@skarzynski.com
• Trevor Ross Fehr trevor.fehr@usdoj.gov

- 1 • Robert David Gallo dgallo@phrd.com
- 2 • Debra I. Grassgreen dgrassgreen@pszjlaw.com, hphan@pszjlaw.com
- 3 • Gail S. Greenwood ggreenwood@pszjlaw.com, rrosales@pszjlaw.com
- 4 • John Grossbart john.grossbart@dentons.com, docket.general.lit.chi@dentons.com
- 5 • John Grossbart , docket.general.lit.chi@dentons.com
- 6 • Joshua K Haevernich joshua.haevernich@dentons.com
- 7 • Robert G. Harris rob@bindermalter.com, RobertW@BinderMalter.com
- 8 • Deanna K. Hazelton deanna.k.hazelton@usdoj.gov
- 9 • Jordan Anthony Hess jhess@plevinturner.com
- 10 • Todd C. Jacobs tjacobs@phrd.com
- 11 • Daniel James daniel.james@clydeco.us
- 12 • Christopher D. Johnson chris.johnson@diamondmccarthy.com
- 13 • Jeff D. Kahane jkahane@skarzynski.com
- 14 • Taylore Karpa Schollard tkarpa@robinskaplan.com
- 15 • Ori Katz okatz@sheppardmullin.com, LSegura@sheppardmullin.com
- 16 • Jeannie Kim jekim@sheppardmullin.com, dgatmen@sheppardmullin.com
- 17 • David S. Kupetz david.kupetz@troutman.com, Mylene.Ruiz@lockelord.com
- 18 • Jennifer R Liakos jenn@jennliakoslaw.com
- 19 • Christina Marie Lincoln clincoln@robinskaplan.com, LCastiglioni@robinskaplan.com
- 20 • Lisa Arlyn Linsky llinsky@mwe.com
- 21 • John William Lucas jlucas@pszjlaw.com, ocarpio@pszjlaw.com
- 22 • Betty Luu bluu@duanemorris.com
- 23 • Alan H. Martin AMartin@sheppardmullin.com,
- 24 • lwidawskyleibovici@sheppardmullin.com
- 25 • Patrick Maxcy patrick.maxcy@dentons.com, docket.general.lit.chi@dentons.com
- 26 • Patrick Maxcy , docket.general.lit.chi@dentons.com
- 27 • Brittany Mitchell Michael bmichael@pszjlaw.com
- 28 • Andrew Mina amina@duanemorris.com
- M. Keith Moskowitz keith.moskowitz@dentons.com
- Michael Norton michael.norton@clydeco.us, nancy.lima@clydeco.us
- Office of the U.S. Trustee / SF USTPRegion17.SF.ECF@usdoj.gov
- Paul J. Pascuzzi ppascuzzi@ffwplaw.com, docket@ffwplaw.com
- Robert J. Pfister rpfister@pslawllp.com
- Mark D. Plevin mplevin@plevinturner.com, mark-plevin-crowell-moring-8073@ecf.pacerpro.com
- Gregory S. Powell greg.powell@usdoj.gov, Tina.L.Spyksma@usdoj.gov
- Douglas B. Provencher dbp@provlaw.com
- Nathan W. Reinhardt nreinhardt@skarzynski.com
- Jason E. Rios jrios@ffwplaw.com, docket@ffwplaw.com
- Kathleen Mary Derrig Rios Katie.Rios@wbd-us.com
- Matthew Roberts mroberts@phrd.com
- Annette Rolain arolain@ruggierilaw.com
- Cheryl C. Rouse rblaw@ix.netcom.com
- Samantha Ruben samantha.ruben@dentons.com
- Phillip John Shine phillip.shine@usdoj.gov
- James I. Stang jstang@pszjlaw.com
- Devin Miles Storey dms@zalkin.com
- Jason D. Strabo jstrabo@mwe.com, dnorthrop@mwe.com

- Catalina Sugayan catalina.sugayan@clydeco.us, Nancy.Lima@clydeco.us
- Edward J. Tredinnick etredinnick@foxrothschild.com
- Miranda Turner mturner@plevinturner.com
- Joshua D Weinberg bkfilings@ruggierilaw.com
- Matthew Michael Weiss mweiss@phrd.com
- Harris Winsberg hwinsberg@phrd.com
- Yongli Yang yongli.yang@clydeco.us

☒ **BY MAIL** I am readily familiar with the business' practice for collection and processing of correspondence for mailing with the United States Postal Service. The address(es) shown below is(are) the same as shown on the envelope. The envelope was placed for deposit in the United States Postal Service at Buchalter in San Francisco, California on **May 1, 2025**. The envelope was sealed and placed for collection and mailing with first-class prepaid postage on this date following ordinary business practices.

SEE ATTACHED MAILING LIST

☒ I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct to the best of my knowledge. Executed on **May 1, 2025**, at San Francisco, California.

☒ I declare that I am employed in the office of a member of the bar of this court at whose direction the service was made. Executed on **May 1, 2025**, at San Francisco, California.

Hallina Pohyar

/s/ Hallina Pohyar
(Signature)

MAILING LIST

Sophia Achermann
605 Market Street, Suite 1103
San Francisco, CA 94105

Marc D. Ashley
Diamond McCarthy, LLP
15 W. 18th St., #1A
New York, NY 10024

C. B.
c/o Kim Dougherty, Esq.
Justice Law Collaborative
210 Washington Street
North Easton, MA 02356

J. B.
c/o Kim Dougherty, Esq.
Justice Law Collaborative
210 Washington Street
North Easton, MA 02356

Blank Rome, LLP
2029 Century Park Est
6th Floor
Los Angeles, CA 90067

R. C.
c/o Kim Dougherty, Esq.
Justice Law Collaborative
210 Washington Street
North Easton, MA 02356

Robin D. Craig
CRAIG & WINKELMAN LLP
2001 Addison Street, Suite 300
Berkeley, CA 94704

J. D.
c/o Kim Dougherty, Esq.
Justice Law Collaborative
210 Washington Street
North Easton, MA 02356

H. F., R. F., D. R., A. S. & R. F. Jr.
c/o Kim Dougherty, Esq.
Justice Law Collaborative
210 Washington Street
North Easton, MA 02356

Felderstein Fitzgerald Willoughby Pascuzzi &
Rios LLP
500 Capitol Mall, Suite 2250
Sacramento, CA 95814

Elise S. Frejka
415 East 52nd St., Ste. 3
New York, NY 10022

GDR Group, Inc.
c/o Robert R. Redwitz
3 Park Plaza, Suite 1700
Irvine, CA 92614

GlassRatner Advisory & Capital Group, LLC
19800 MacArthur Blvd.
Irvine, CA 92612

Jordan A. Hess
Crowell & Moring LLP
1001 Pennsylvania Ave.
Washington, DC 20004

Kern County Treasurer and Tax Collector
Office
Attn: Bankruptcy Division
P.O. Box 579
Bakersfield, CA 93302-0579

Matthew C. Lovell
Nicolaides Fink Thorpe et al
101 Montgomery St., # 2300
San Francisco, CA 94104

Lauren M. Macksoud
Dentons US LLP
1221 Avenue of the Americas
New York, NY 10020-1089

Rosalle Marcic
c/o Jeannette A. Vaccaro, Esq.
315 Montgomery St. 10th Floor
San Francisco, CA 94104

Brittany M. Michael
PACHULSKI STANG ZIEHL & JONES LLP
780 Third Avenue, 34th Floor
New York, NY 10017-2024

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Geoffrey M. Miller Dentons US LLP 1121 Avenue of the Americas New York, NY 10020-1089	Fr. Patrick Summerhays The Roman Catholic Archbishop of SF One Peter York Way San Francisco, CA 94109
Omni Agent Solutions 5955 De Soto Avenue, Suite 100 Woodland Hills, CA	Transperfect Legal Solutions 1250 Broadway New York, NY 10001
Alexander Potente CLYDE & CO US LLP 150 California Street, 15th Floor San Francisco, CA 94111	Miranda H. Turner Crowell & Moring LLP 1001 Pennsylvania Avenue, N.W. Washington, DC 20004
Cristopher W. Ray McDermott Will & Emery LLP One Vanderbilt Ave. New York, NY 10017	Weinstein & Numbers, LLP 115 Ward Street Larkspur, CA 94939
Damion D. D. Robinson 355 South Grand Avenue, Suite 2450 Los Angeles, CA 90071	Weintraub Tobin Chediak Coleman & Grodin 475 Sansome St. San Francisco, CA 94111
Russell W. Roten Skarzynski Marick & Black LLP 633 West Fifth Street, 26th Floor Los Angeles, CA 90071	Carole M. Wurzelbacher McDermott Will & Emery LLP 444 W. Lake St., #4000 Chicago, IL 60606

EXHIBIT A

April 28, 2025

BRG Incident Update

This letter is intended to provide information regarding a recent cybersecurity incident (the “Incident”) at Berkeley Research Group, LLC (“BRG”), which was discovered on March 2, 2025 when BRG detected suspicious activity in its network.

Upon detection, BRG immediately launched an investigation, through which it confirmed that specific BRG internal systems were impacted by ransomware. BRG immediately deployed containment measures, engaged outside counsel at Octillo Law PLLC, who in turn engaged expert security and forensics specialists at Booz Allen Hamilton, and alerted the FBI. The Incident is described further in the FAQs set forth at the end of this letter, along with the investigation findings summary sent alongside this letter, which includes an attestation from BRG’s third-party forensics firm affirming the Incident is contained and the threat actor has been expelled from our environment.

After careful consideration, and with a primary focus on protecting the subjects of any implicated data, BRG reached a settlement with the threat actors to attempt to mitigate harm and prevent any distribution of the data. While statements from threat actors may not be 100% reliable, the threat actor has represented that any data exfiltrated / stolen during the Incident has since been deleted.

Since BRG’s discovery of the Incident, BRG has been conducting a thorough analysis to understand the scope of potentially exfiltrated data, which remains ongoing and will require significant time to complete. That said, we want to be prompt about providing information that is important to you as we learn of it along the way, with the caveat that we may need to update or amend this information as our investigation progresses.

To that end, our investigation has identified that data associated with *In re The Roman Catholic Archbishop of San Francisco* (the “Subject Case”) appears to have been exfiltrated by the threat actor in the course of the Incident. As discussed above, the threat actor has represented the exfiltrated data associated with this case has since been deleted.

With assistance from professional data experts, we are actively and thoroughly investigating whether this data included (a) any identifiable information, even if it is just a name, relating to individuals involved in the Subject Case or (b) any information subject to a protective order or confidentiality agreement. We will provide more details as our data analysis and investigation proceeds, including the scope of any data exfiltrated and steps BRG will take to help satisfy any statutory or contractual notice requirements.

BRG understands that there are court orders related to the Subject Case that must be addressed. BRG has engaged bankruptcy counsel to assist in this process and plans on notifying the presiding Court of this matter in the Subject Case promptly.

We thank you in advance for your patience as we continue to address this matter, and we ask that you reach out to us at DataAnalysisInquiries@thinkbrg.com with any questions or requests.

Thank you,

Berkeley Research Group, LLC

BRG IT Security Incident FAQs

Incident Background and Response Efforts

Q: When did the incident occur, when was it contained, and when was BRG able to confirm that the threat actor no longer had access to BRG systems?

A: On Sunday, March 2, 2025, BRG detected suspicious activity in its network and immediately launched an investigation, through which it confirmed that specific BRG internal systems were impacted by ransomware. Further investigation identified that the Incident began on February 28, 2025, when a Threat Actor socially engineered a BRG employee to obtain remote access to their laptop. The BRG employee was not a member of the team that works on the Subject Case. Specifically, the Threat Actor placed a phone call to this BRG employee posing as BRG IT support. BRG uses VoIP phone systems for external calls that ring similarly to internal MS Teams calls. Note, however, that there is no evidence that the Threat Actor was inside BRG's Teams instance. The employee allowed those posing as BRG IT support to establish remote access to their laptop.

BRG provides in-depth and frequent training to its employees regarding social engineering risks. Unfortunately, common human characteristics such as a tendency to trust those with seeming authority, susceptibility to claims of urgency, lack of skepticism about what seems familiar, and basic human error all mean that almost anyone can fall for a well-executed social engineering attack.

Q: What did BRG do to contain the incident?

Upon discovering the Incident, BRG immediately deployed containment measures, engaged outside counsel and expert security and forensics specialists at Booz Allen Hamilton, and alerted the FBI and insurance carriers. BRG's immediate containment measures included taking systems offline proactively to mitigate the spread of any residual threat actor activity and enhancing endpoint threat detection by deploying SentinelOne.¹ More specifically, BRG and Booz Allen took the following measures:

- **Disconnecting all inbound and outbound connections**
- **Rotating credentials for every user, account, and system using out-of-band resetting procedures**
- **Reset Kerberos credentials and repeating reset according to incident response best practices**
- **Auditing Active Directory for any recent modified or new accounts**
- **Disabling accounts potentially used by the Threat Actors**

¹ SentinelOne is a premier Endpoint Detection & Response solution that provides advanced threat detection and automated response capabilities.

- Auditing global policies
- Auditing BRG's MFA provider, MS Authenticator, to ensure no new accounts were created

Q: What type of threat detection system did BRG have in place during the Incident?

A: BRG has Microsoft Defender for Endpoint as its Endpoint Detection and Response (EDR) system. An EDR system is a cybersecurity technology designed to continuously monitor and respond to threats on endpoints, such as computers and servers. Microsoft Defender for Endpoint uses AI and machine learning to monitor endpoints for suspicious activities and potential threats continuously. It can detect malicious behavior and indicators of compromise (IOCs) and alert and respond to environmental threats. BRG also has a full-time, managed services Security Operations Center (SOC) that monitors BRG's environment around the clock and responds to alerts such as those provided by Microsoft Defender for Endpoint. Since the Incident, BRG has supplemented its typical SOC with incident response team members. The threat actor was able to evade EDR detection by using tools that would be authorized in a standard technical environment and not trigger alerts, known as "living off the land."

Q: Did BRG deploy an End-Point Detection and Response ("EDR") tool (e.g., Carbon Black, SentinelOne, CrowdStrike Falcon)?

A: Yes, BRG deployed SentinelOne after the incident was discovered in addition to the existing implementation of Microsoft Defender for Endpoint.

Q: Has BRG contacted law enforcement?

A: Yes. The FBI has been engaged.

Investigation Findings

Q: What was the attack vector?

A: The attack vector was a new Chaos ransomware variant. A list of indicators of compromise is set forth in the investigation findings report we are providing to you alongside this letter.

Q: Was any data exfiltrated (or stolen)?

A: We have confirmed that data was exfiltrated. We have also identified that information related to the Subject Case appears to be within that exfiltrated data, and we are conducting further data analysis to identify any individuals whose name or other information was contained therein.

Q: Is there a risk that malware or other malicious files could have been transmitted to third parties? Please describe.

A: No, our investigation has not identified any evidence to suggest this occurred, and no BRG clients have indicated they were compromised because of this incident.

Q: Did the threat actor demand a ransom and if so was it paid?

A: After careful consideration, and with a primary focus on protecting the subjects of any implicated data, BRG reached a settlement with the threat actors to attempt to mitigate harm and prevent any distribution of the data.

Q: Has the threat actor threatened to leak or disclose data?

A: The threat actor advised us that they have deleted the data and will not leak or disclose it.

Q: How do you know that the threat actor has deleted the data and will not further disclose it?

A: We recognize that statements from threat actors cannot be considered 100% reliable, but they have provided BRG with a destruction log and stated that any data exfiltrated during the Incident has since been deleted and will not be disclosed further. Additionally, threat actors of this nature are believed to follow through on these kinds of statements because (a) continuing to retain data is costly and it is not worthwhile for them to devote resources towards that; and (b) failing to follow through on these statements undercuts their business model and signals to future victims that there is no reason to negotiate with them. Lastly, BRG has conducted and continues to conduct dark web monitoring and, to date, has not seen any indications to suggest data has been leaked or disclosed in connection with this incident.

Data Analysis and Next Steps

Q: Was any data associated with the Subject Case exfiltrated?

A: Yes, based on our review of the impacted data and our mapping of where certain matter data is stored, we have determined that data associated with Subject Case appears to have been exfiltrated.

Q: Was any PII or names of individuals involved in the Subject Case exfiltrated?

A: We are conducting further data analysis to answer this question. In the event we identify any such impact to PII or names of individuals involved in the Subject Case, we will notify you accordingly.

Q: Was any information covered by protective orders in the Subject Case exfiltrated?

A: We are conducting further data analysis to answer this question. In the

event we identify any such impact to information covered by protective orders, we will notify you accordingly.

Q: If you determine that PII or names of individuals involved in the Subject Case was exfiltrated, what steps will you take?

A: After first notifying you of our findings, we will then be prepared to provide notification to individuals and/or regulatory authorities as required by state and federal notification laws, unless you advise us that you would like to provide those notifications.

Q: If you determine that information covered by any protective orders in the Subject Case was exfiltrated, what steps will you take?

A: After first notifying you of our findings, we will then be prepared to notify the Court.

Q: Will BRG provide more information when its investigation is complete?

A: Yes, we will provide further information to you regarding impacted data associated with the Subject Case once our data analysis and investigation has concluded.



octillo
LEGAL + TECH

Investigation Findings Summary

Berkeley Research Group

April 2025

Overview

This document serves as the investigation findings summary for Berkeley Research Group ("BRG") in relation to a cybersecurity incident detected by BRG on March 2, 2025 (the "Incident"). The document was prepared by Octillo Law PLLC ("Octillo") in furtherance of their legal counsel and is based on the findings observed by Booz Allen Hamilton ("Booz Allen"), the forensic specialist and incident response firm retained by Octillo to conduct an investigation into the Incident.

Findings – Executive Summary

On March 2, 2025, BRG engaged cybersecurity professionals, including Octillo as counsel and forensic specialists at Booz Allen Hamilton ("Booz Allen"), following the identification of unauthorized activity consistent with a ransomware attack, which was later identified to be associated with a new variant of Chaos ransomware.¹ Upon discovering the Incident, BRG immediately deployed containment measures, including taking systems offline proactively to mitigate the spread of any residual unauthorized activity and enhancing endpoint threat detection by deploying SentinelOne. Containment of the Incident was confirmed by Booz Allen and there have been no alerts of suspicious activity within BRG's environment since March 2, 2025.

BRG identified that the Incident initially began on February 28, 2025, when an unauthorized actor ("UA") placed a phone call to a BRG employee posing as BRG IT support and the employee allowed remote access to their laptop at the UA's request. While the phone call appeared to the employee to be an internal Microsoft Teams call, further investigation confirmed that this call by the UA originated outside of BRG's environment, as BRG uses VoIP phone systems for external calls that ring similarly to internal Microsoft Teams calls, and there is no evidence that the UA was inside BRG's Teams instance. Further investigation determined that, although BRG had Microsoft Defender for Endpoint and a 24/7 SOC in place prior to the Incident, the UA leveraged tools authorized in BRG's environment in a manner designed to evade detection. The investigation determined that there was no evidence of unauthorized access to BRG's Microsoft Office 365 environment (email, OneDrive, OneNote, Teams, SharePoint), nor to BRG DRIVE, BRG Symphony, Second Sight, Azure, AWS or Kiteworks.

As described in more detail below, BRG's investigation determined that the UA escalated privileges before moving laterally inside BRG's environment and deploying ransomware that encrypted some BRG systems. Additionally, the investigation also identified indications of data exfiltration. In light of these findings, BRG is engaged in further data analysis to understand the full scope of regulated data impacted by the Incident. At present, BRG is not aware of any identify theft or fraud stemming

¹ This new Chaos ransomware variant is not the same as that used by the cybergang Ryuk in the early 2020s, for which decryption keys are publicly available.

from this Incident and, similarly, BRG's ongoing dark web monitoring has not identified any indications that information related to this Incident has been posted on the dark web.

Findings – Unauthorized Activity

February 28, 2025

18:10 – 18:34 UTC

- The UA places a phone call to a BRG employee ("Employee A") that rings through Microsoft Teams ("Teams"), posing as a member of BRG IT Support and requesting remote access to the employee's laptop.
- Employee A executes QuickAssist.exe and Anydesk.exe at the UA's direction, thereby allowing remote access to their laptop.
- UA sets up a Qemu virtual machine ("Qemu VM")² on Employee A's account, using tools that would be authorized in a standard technical environment and not trigger alerts.

18:37 UTC

- First observed logon using Anydesk.exe by the UA on Employee A's account from IP address 185.33.87[.]67.

19:41 UTC

- UA conducts Kerberoasting³ using Employee A's local account to obtain privileges for the Local Administrator Account.

21:42 – 21:57 UTC

- UA places a phone call to a separate BRG employee ("Employee B") that rings through Teams, again posing as a member of BRG IT support and requesting remote access to their laptop.
- UA sets up a Qemu VM on Employee B's account, Employee B downloads QuickAssist.exe at UA's direction, and UA visits <https://1ty.me/x0erIMy>, a self-destructing link for sharing information.

² Qemu VM is a standard tool commonly used for penetration testing, but was leveraged by the UA for malicious purposes during the Incident.

³ Kerberoasting is a technique targeting the Kerberos authentication protocol, enabling unauthorized actors to extract encrypted account credentials.

22:17 – 22:19 UTC

- UA leverages the Local Administrator Account privileges obtained through the Kerberoasting to move laterally from Employee B's account to a BRG domain controller.
- UA creates and executes remote management tools on the domain controller using a Domain Administrator Account.

23:38 UTC – 3/1/2025 03:22 UTC

- UA conducts network reconnaissance to 18 different hosts.

March 1, 202506:00 – 07:13 UTC

- UA executes remote management tools on the Qemu VM from Employee B's account.
- UA makes lateral movement to a separate BRG domain controller.

07:01 – 09:13 UTC

- Using the Domain Administrator Account, the UA conducts lateral movement to additional systems within BRG's network.
- UA harvests credentials and escalates privileges by accessing memory on one of the impacted systems and conducts additional network reconnaissance.
- UA clears system logs and the Administrator Security Log on one of the impacted systems using the Domain Administrator Account.
- UA executes PowerShell commands to search for "backup files"; "Defender for endpoint status"; "server versions"; and "sensitive files". Files were created and then deleted by the UA.

09:45 – 3/2/2025 06:52 UTC

- UA conducts lateral movement to additional systems in BRG network.

March 2, 202506:39 – 09:15 UTC

- File and directory access and data compression and staging by the UA on multiple systems.

07:08 – 11:00 UTC

- UA leverages additional tools and runs commands aimed at further network reconnaissance in advance of ransomware encryption.
- UA conducts additional log clearing of Windows Event Logs.

12:05 UTC

- UA obtains additional account credentials from a VeeamBackup Database on impacted systems.

12:53 – 13:27 UTC

- UA begins deployment of ransomware encryption with extension “.chaos” and the ransom note readme.chaos.txt is placed on multiple systems.

13:31 – 21:25 UTC

- UA performs lateral movement to one additional system and creates a new user account before disconnecting from BRG network.

Indicators of Compromise

Based on the investigation, BRG and Booz Allen identified the following indicators of compromise:

Binary / IP Address	Hash
185.33.87[.]67	
88.119.167[.]239	
socks.exe	MD5: 9d126f26bc3fe620319944a6f64c6906 SHA-1: 8ce752408fff84d2a621c4dac61067fb0a750a32 SHA256: 073874a38fb63387ab9f9b592dab5e49c6407fb899c11f8b7859334a219aeced
w.exe	MD5: 8697ff6c68e4d029b4980fed99f3ff96 SHA-1: 8deadd1aca25ccf867f2b1b2781d1e665359e31e SHA-256: af68dfd0ad3d95ff0869b593289eff4c26f5a6a2793b441010c51da891b58269
ScreenConnect.ClientService.exe	SHA256: dc936234f0d802cb91ab9653f0ab4b401d4e64a9cad5080f767d748db479716c
start.txt	SHA256: 89709925b4ec3aefe93de07585b06acb9721e69517525009e2a7534b2bb69f73
SyncroLive.Service.exe	MD5: b025ef996de7a7c4d772721bc5ed2eba SHA-1: 2749ee05cd22819dc70f9f988d37f7c252c477bc SHA-256: 132677d3e6ec1e0f46844c6b7b0a5383ca98b9384e9d8002c7a42535b74ebe57
SyncroLive.Agent.exe	MD5: bde70df2c0087aec6c76697086fa0d78 SHA-1: ca9ff91dad4c31bdca0800e680ad1b0d78789a57 SHA-256: 0e54383b5b92f27dfbc80e9c811bd5973f8ddd93bb52c68565f455b189e8986c
Update.vbs	SHA256: c7e3603d04c0452da1199593322b5a8ca0f6d849ccdd77287d0511c71cef466f

Binary / IP Address	Hash
rcclone.exe	MD5: 316a534a8f17de17c38ee3f7c37eedf4 SHA-1: 3511c07428fef55e2ff2f3b38442a91b6422e10b SHA-256: c189595c36996bdb7dce6ec28cf6906a00cbb5c5fe182e038bf476d74bed349e
Update.qcow	MD5: 0866e529ef49ac2248d4c2d97d317112 SHA1: c3e2665ab8303b44ba4bd647be976129241098c1 SHA256: 2b6ea41a9807dd7cf2164b5a896a638acde773a037e0f7531b311648bd9ef34f
prevercheck.exe	MD5: 2c18826adf72365827f780b2a1d5ea75 SHA-1: a85b5eae6eba4af001d03996f48d97f7791e36eb SHA-256: ae06a5a23b6c61d250e8c28534ed0ffa8cc0c69b891c670ffaf54a43a9bf43be
1.bat	
2.bat	
1 - copy.bat	
soc.exe	SHA-1: 6ff66452e1ea940e1089ba961fad6cecc9c43731
1.exe	
Netscan.exe	

Containment & Eradication

In response to this incident, BRG immediately brought systems within their environment offline to mitigate the spread of any residual UA activity. Additionally, BRG implemented enhanced endpoint threat detection by having SentinelOne deployed to all systems within the environment. Active monitoring for threats is ongoing. More specifically, BRG and Booz Allen took the following measures:

- Disconnecting all inbound and outbound network connections;
- Rotating credentials for every user, account, and system using out-of-band resetting procedures;
- Reset Kerberos credentials and repeating the reset according to incident response best practices;
- Auditing Active Directory for any recent modified or new accounts;
- Disabling accounts potentially used by the UA;

- Auditing global policies;
- Auditing BRG's MFA provider, MS Authenticator, to ensure no new accounts were created.

There has been no observed recurrence of unauthorized access to endpoints within the BRG environment following containment and eradication, and an attestation of containment from Booz Allen is attached to this report.

Additional Improvements

Following its initial containment and eradication efforts, BRG undertook further investigation to explore additional opportunities aimed at enhancing its already robust security measures and practices, including the following:

- Implemented a tiered Microsoft Active Directory structure, thereby establishing segregation of duties to minimize the risk of privilege escalation, credential theft, and lateral movement within an IT environment. This model consists of three security tiers, each with specific responsibilities and access controls:
 - Tier 0 – Privileged Access: Direct control over identity, authentication, and security infrastructure.
 - Tier 1 – Enterprise Servers & Applications: Controls application and server resources (e.g., Exchange, SQL, and line-of-business applications).
 - Tier 2 – User Workstations & Productivity: Controls standard user devices and environments.
- Removal of VMware and Storage appliances from the Microsoft Domain.
- Passwords for all user, service, and administrative accounts in the domain have been changed twice, including Kerberos (krbgt).
- Establishment of "Honeypot" accounts – placed certain accounts in a group that alerts BRG when they are used.
- Reviewed and hardened all Group Policies within the BRG Domain.
- Enhanced its pre-Incident EDR measures by increasing the monitoring and reporting of Microsoft Defender for Endpoint and BRG's External SOC.
- Performed a policy review and upgraded all Palo Alto Firewalls to the latest firmware and software levels.
- Enhanced authentication measures for calls received from BRG IT to reduce the risk of social engineering.

To: Whom it May Concern
From: Booz Allen Hamilton
Ref: Berkeley Research Group
Date: March 13, 2025

On March 2, 2025, Berkeley Research Group (BRG) experienced a cybersecurity incident involving a user that was socially engineered which led to the deployment of ransomware and encryption of data. Booz Allen Hamilton (Booz Allen) was engaged by BRG's counsel to assist in responding to the incident.

Booz Allen is a consulting firm which specializes in digital forensics and incident response, handling numerous ransomware, malware, and business email compromise (BEC) investigations per year. Booz Allen provides a full suite of incident response services including digital forensic investigations, incident containment, restoration and recovery services, threat hunting and Endpoint Detection and Response (EDR) monitoring.

In support of the investigation the Booz Allen Threat Detection and Response (TDR) team worked with the Berkeley Research Group team to deploy an EDR tool (SentinelOne) to all systems including high-value target servers and computer endpoints within the environment and have confirmed 100% saturation. Threat hunting has been performed daily, and continuously, through the date of this letter, specifically to identify suspect binaries and executions both current and historical based on the available evidence. Any indicators of compromise identified as result of the forensic investigation were re-mediated and added to be banned within the SentinelOne EDR platform. At this time, Booz Allen has not observed further activity by any unauthorized person or malicious and suspicious files in the BRG environment following the incident. In addition, and according to security best practices, The Booz Allen team with support from the BRG team undertook a series of decisive and comprehensive measures to enhance security and resilience:

1. **Deployment of SentinelOne:** SentinelOne was deployed with 100% coverage and monitored 24/7. Its playbook was enhanced with indicators of compromise from this engagement as well as previous ones, ensuring comprehensive protection.
2. **Global Password Reset:** A global reset was conducted for all user, administrator, and service account passwords. The Kerberos ticketing account, used for Windows environment authentication, had its password changed twice initially and once more after twelve hours to eliminate any cached or clear-text credentials.
3. **Compromised User Account:** The affected user account had its password reset and was then disabled. A new account was created to replace the compromised one.
4. **Active Directory Audit:** The Active Directory was thoroughly audited to identify any suspicious accounts or unauthorized changes. No evidence of such activity was found.
5. **Group Policy Audit:** An audit of Group Policies was conducted to detect any unauthorized changes or newly created policies, with none identified.

By: 

Name: Brendan Rooney

Title: Senior Vice President